ASSIGNMENT - 13

Dr. GVL Prasad

(1) What is TOR and discuss attacks that are possible on it. Install TOR on your system and compare and contrast it with a regular search engine like google.

Ans TOR (The onion Router) is a free and open-source software that anonymizes your internet traffic. It achieves this by routing your communication through a network of volunteer-run servers around the world, encrypting it layer by layer like an onion. This makes it difficult to trace a user's activity back to its source.

Here are some attacks that are possible on TOR:-

Traffic analysis attacks: By analyzing the flow and timing of data packets, attackers can potentially infer information about the user's activity, even if the content is encrypted.

Exit node attacks:- The exit node is the last server in the TOR chain that communicates with the internet. A malicious exit node could potentially steal information or manipulate data.

Browser vulnerabilities:- Malicious websites or browser extensions could exploit vulnerabilities to de-anonymize users.

How TOR Differs from a regular search engine (like Google)

Feature	TOR	Regular search Engine like Google
Purpose	Anonymize internet traffic	Find information on the internet
Anonymity	High	Low (Tracks user data)
Security	Moderate (vulnerable to attacks)	Low (vulnerable to hacking)
Content access	Access some Hidden websites	Access the entire internet

In short:-

- Use TOR if you prioritize anonymity and privacy over speed and content access.
- Use a regular search engine if you prioritize finding information quickly and easily.

Additional Tips:-

* Even with TOR, it's important to be aware of your online behaviour and practice good security habits.
* Consider using TOR in conjunction with a VPN for additional security.

(3) What are deepfakes? Discuss how they are being used for impersonation attacks. Explain how they can be countered.

Ans:- Deepfakes are synthetic media, typically videos or audio recordings, that have been manipulated using AI to make them appear real. They can be used to convincingly replace a person's face or voice with someone else's.

Impersonation attacks with deepfakes:

Malicious actors are increasingly using deepfakes to impersonate real people in cyberattacks. With deepfakes, here are some methods.

Social Engineering: Deepfake videos or audio recordings can be used in phishing scams.

Business mail compromise (BEC): Attackers can use deepfakes to impersonate executives or high-level employees via email. These emails might instruct employees to transfer funds or share confidential data.

Discrediting Individuals: Deepfakes can be used to create compromising or damaging videos or audio of people, potentially harming their reputation.

Countering deepfake attacks:

While deepfakes are becoming more sophisticated, there are ways to counter them.

Awareness training.
Multifactor authentication
Technical Detection tools.
Regulation & Legislation.
By staying informed and implementing these measures we can help mitigate the threat of deepfake attacks.

(4) Discuss about different types of cyber crimes. Explain how person can report to the concerned officials and take protection.

Ans: Cybercrime encompasses a vast range of criminal activities that exploit computers, networks and digital devices. Here's a breakdown of some common types.

* Financial crimes.
* Identity Theft.
* Malware Attacks.
* Data Breaches.
* Social Engineering.
* cyberstalking & Harassment.
* cyberespionage.
* Denial of service (DOS) attacks.
* cyberbullying.
* Software Piracy.

Reporting cybercrime:-
If you become a victim of cybercrime, here are some steps to take.

1. Collect evidence.
2. Report to law enforcement.
3. Report to relevant Authorities.
4. Report to platform.

Protecting yourself:-
Here are some ways to minimize your risk of cybercrime.

(1) Strong passwords & multi. factor authentication

(2) Software updates.
(3) Beware of phishing
(4) Data backups.
(5) Antivirus and anti malware software
(6) Be wary of free downloads.
(7) Social media Privacy settings.

By staying informed and practicing good cybersecurity habits, you can significantly reduce your risk of becoming a victim of cybercrime.

5. Discuss about various online payment frauds and how can they be prevented?

Ans: Online payment fraud is a growing concern as more and more transactions move online. These scams aim to steal your financial information, money or both. Here's a breakdown of common types online payment fraud and how to prevent them.

Types of online fraud:-

(1) Phishing scams.
(2) Data breaches
(3) Card not present (CNP) fraud.
(4) Identity theft.
(5) Friendly fraud.

Preventing online payment fraud:-

(1) Be wary of phishing.
(2) Strong passwords + Multi-factor authentication
(3) Secure websites
(4) Review Bank statements regularly.
(5) Beware of public wi-fi
(6) Use secure payment methods.
(7) Scrutinize online marketplaces.
(8) Beware of unrealistic deals.

By following these precautions and staying vigilant, you can significantly reduce your risk of falling victim to online payment fraud.